REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1-56 are pending. Claims 1, 13, 23, 30, 42, 48, and 53 are in independent form. No claim amendments are proposed at this time.

Applicant gratefully acknowledges the Examiner's consideration of the reference cited on the Form PTO-1449 filed November 21, 2000 and return of the initialed Form.

In the action mailed June 1, 2004, claims 1-56 were rejected as obvious under 35 U.S.C. § 103(a). The rejections of the claims rely upon various references relating to bank and credit card account transactions, either alone or in combination with United States Patent No. 6,105,010 to Musgrave (hereinafter "Musgrave").

The rejection alleges that it would have been obvious to apply known security/authorization processes to the biometric certificates of Musgrave or to other digital security mechanisms associated with a user's identity.

Despite the assertion on page 4, paragraph 10 of the Office action to the contrary, Applicant submits that the application of known security/authorization processes to digital security mechanisms associated with a user's identity is not obvious. In

support of this contention, attention is directed to Musgrave itself.

In particular, Musgrave fails to describe or suggest storing a result of a verification of a digital credential in a central service and allowing specified users to access the result. Rather, in Musgrave, once a verification message is transmitted by biometric verification processor 22, biometric verification processor 22 does not appear to perform further activities. In other words, there is no indication in Musgrave that biometric verification processor 22 stores a record of the result of the verification in a central service, nor does biometric verification processor 22 allow specified users to access these results.

This interpretation of Musgrave is not supported. There is a complete absence of any description or suggestion that Musgrave's biometric verification processor performs these acts. Moreover, there is a description that Musgrave's biometric verification processor is preferably incorporated into a data provider or electronic transaction processor (as described at col. 3, line 6-10). When the biometric verification processor is incorporated into a data provider or electronic transaction processor, there is no central service to store a record of the result of the verification of Musgrave's biometric certificates.

Indeed, such an incorporated biometric verification processor may be incapable of receiving a request to verify a use of a digital credential at a first of a plurality of different services where the digital credential can be used.

Thus, the only implementation of Musgrave that is not expressly precluded from storing a record of the result of the verification in a central service is the implementation where Musgrave's biometric certifying authority handles transactions between other entities such as banks and consumers (as described at col. 3, line 13-18). In this implementation, there is simply no description or suggestion that the biometric verification processor stores a record of the result of the verification in a central service or allows specified users to access these results.

As discussed in the response filed March 19, 2003, this combination of Musgrave's biometric system with financial account transaction systems (such as those described in Anderson, Vance, Goldsmith, Yacobi, and Sudia) is the only art of record describing a combination of Musgrave with account transaction systems. In this combination, Musgrave's biometric certification process operates in a manner that is distinct from the manner in which traditional account transaction systems operate.

In particular, Musgrave's biometric certification process is to occur as a counterpart to bank and credit card account transaction systems. In this counterpart operation, there is no storage of a record of the result of the verification of Musgrave's biometric certificates. Rather, transaction record keeping appears to occur at the account level, just as described in Anderson, Vance, and the other art of record.

This counterpart operation is thus different from the present claims. In particular, with this counterpart operation, there is no description or suggestion regarding storing a result of a verification of a digital credential associated with a user's identity in a central service or allowing specified users to access these results.

Therefore, the combination of Musgrave and the other references fails to describe or suggest elements and limitations recited in the claims, and a *prima facie* case of obviousness has not been established. Further, there is no support for the contention that the application of known security/authorization processes to digital security mechanisms associated with a user's identity is obvious, since the only art of record demonstrates operation without such an application.

The rejection contends that this line of reasoning amounts to improperly attacking the references individually when the

rejection is based upon the teachings of a combination of references. However, none of the cited art describes or suggests the identified claim elements and limitations. Thus, the combined teachings of the references would not have suggested such elements and limitations to those of ordinary skill in the art. Applicant is thus not attacking the references individually, but rather pointing out a deficiency in the combination as whole.

The rejection thus amounts to an unsupported conclusion that it would have been obvious to apply known security/authorization processes to digital security mechanisms associated with a user's identity (such as the biometric certificates of Musgrave). For example, on page 4, paragraph 12, it is contended that a notification procedure would occur regardless of whether account information were verified or a digital security mechanism associated with a user's identity were verified. However, there is no support for this conclusion on the record or founded anywhere in the art of record.

Instead, the scope and content of the art of record indicates that digital security mechanism verifications are to be treated differently from account verifications. For example, Musgrave treats these verifications differently. In particular, Musgrave fails to describe or suggest storing a result of a

verification of a digital credential associated with a user's identity in a central service and allowing specified users to access these results. As another example, the usage of a credit card, discussed in an earlier Office action, treats the verification of account information (e.g., an account number encoded in the card) differently from the verification of security mechanism associated with a user's identity (e.g., a signature, name, or photo). In particular, there is no storage of the result of the verification of a signature, name, or photo in a central service, nor are specified users allowed to access the result.

The mere fact that the claims were within the capabilities of one of ordinary skill is not sufficient to establish a *prima facie* case of obviousness. "Rather, particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed." *In re Kotzab*, 217 F.3d 1365, 1371 (Fed. Cir. 2000).

In the present case, it is respectfully submitted that the Office has not carried its burden of proof and shown why one of ordinary skill would apply known security/authorization processes to biometric certificates or other security mechanism's associated with a user's identity. With all due

respect, the unsupported assertion that such application would occur amounts to improper, hindsight-based reconstruction of Applicant's claims.

Independent Claims 1, 13, and 23

Turning to the individual rejections, independent claims 1, 13, and 23 were rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,021,202 to Anderson et al. (hereinafter "Anderson") and U.S. Patent No. 6,442,526 to Vance et al. (hereinafter "Vance") in view of Musgrave.

The rejection contends that it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the security/authentication process of Anderson with the biometric certification process of Musgrave in order to enhance the security of a transaction. Applicant does not dispute this contention - in fact, Musgrave himself describes that his biometric certification process operates in combination with account transaction processes.

However, Applicant submits that this combination does not describe or suggest the elements and limitations recited in the claims. Claim 1 relates to a method that include storing the result of the verification of a digital credential in an activity log in a central service and allowing specified users

to access the result. As discussed above, none of Musgrave, Anderson, or Vance describe or suggest such a method.

Claim 13 relates to a computer-readable medium having instructions for causing a computer to store a result of a verification of a digital credential in an activity log and to allow specified users to access the result. As discussed above, none of Musgrave, Anderson, or Vance describe or suggest such instructions.

Claim 23 relates to a system including an activity log coupled to the server to store results from verifications of a digital credential and a communication part to allow specified users to access the results. As discussed above, none of Musgrave, Anderson, or Vance describe or suggest such a system.

Musgrave's system operates as a counterpart to a tradition account transaction system where account information in verified and the results of the verification of the account information are stored. There is no reason to believe that one of ordinary skill would change the operation of such traditional account transaction systems upon learning of Musgrave's biometric certificates, nor is there any reason to believe that one of ordinary skill would suddenly handle Musgrave's biometric certificates in the same manner that transaction systems handle account information.

Further, any rejection under 35 U.S.C. § 103(a) that relies upon Musgrave would have to overcome Musgrave's express teachings as to how biometric certificates are to be combined with traditional account transaction systems and hence away from the claimed invention. Without a suggestion or motivation as to the claimed invention, obviousness has not been established.

Since elements and limitations from each of independent claims 1, 13, and 23 are neither described nor suggested by the cited art, it is respectfully submitted that a *prima facie* case of obviousness has not been established. Further, it is respectfully submitted that any *prima facie* case of obviousness relying on Musgrave is, in general, improper given the teachings in Musgrave away from the claims. Accordingly, it is respectfully submitted that claims 1, 13, and 23, and the claims dependent therefrom, are allowable.

Independent Claim 30

Independent claim 30 was rejected under 35 U.S.C. § 103(a) as obvious over Anderson, Vance, and Musgrave. Claim 30 relates to a method that includes receiving use information describing a first use of a digital credential by an owner of a digital credential, receiving use information describing a second use of the digital credential by a delegate of the owner of the digital

credential, storing the use information in an activity log, and generating an activity report for the delegate based on the activity log.

Applicant respectfully traverses the rejection. None of Anderson, Vance, and Musgrave describe or suggest storing use information of a digital credential associated with a the owner's identity in an activity log and generating an activity report based on such an activity log. As discussed above, Musgrave's biometric certification process is to operate distinctly and as a counterpart to traditional account transaction systems. In this counterpart operation, there is no storage of use information of a digital credential associated with the owner's identity in an activity log. Rather, it appears that account use information is to be stored—just as described in Anderson, Vance, and the other art of record.

In addition to these deficiencies, Applicant also submits that the combination of Anderson, Vance, and Musgrave fails to describe or suggest receiving use information describing a first use of a digital credential by an owner of a digital credential and receiving use information describing a second use of the digital credential by a delegate of the owner of the digital credential. Musgrave deals with biometric certificates. Referring to U.S. Patent No. 6,310,966 to Dulude (hereinafter

"Dulude"), which names Clyde Musgrave as a joint inventor and incorporates by reference the same U.S. Provisional Patent Application Serial No. 60/046,012, biometric certificates may be generated using biometric data from a biometric input device. Such biometric data includes fingerprints, hand geometry, iris and retinal appearance, and speech patterns. See, e.g., Dulude, col. 4, line 25-61.

Since Musgrave's biometric certificates are generated using biometric data derived from the physical characteristics of a single individual, Applicant respectfully submits that Musgrave not only fails to describe or suggest but also teaches away from any activity related to use of a digital credential by a delegate of the owner. In particular, unless the delegate were to evade the purpose of Musgrave's system and copy the physical characteristics of the owner of the biometric certificate, then Musgrave's biometric certificates cannot be used by a delegate at different services without frustrating Musgrave's system.

It is therefore respectfully submitted that the rejection does not establish a *prima facie* case of obviousness. Accordingly, it is respectfully submitted that claim 30, and the claims dependent therefrom, are allowable.

Independent Claim 42

Independent claim 42 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,064,990 to Goldsmith (hereinafter "Goldsmith").

Claim 42 deals with a method that includes storing use information for a digital credential of a plurality of delegates who are delegated to use the digital credential by an owner, processing the use information for each of the delegates to detect misuse, and generating an alert to the owner based on the detection of misuse. The digital credential is a digital security mechanism associated with the owner's identity.

The rejection admits that Goldsmith does not relate to digital credentials associated with a user's identity. However, the rejection also contends that it would have been obvious to apply Goldsmith's account activity techniques to digital credential usage information.

Applicant respectfully disagrees with the contention and moreover submits that a *prima facie* case of obviousness cannot be established independently of the scope and content of the prior art. Without *some* support for the contention that the application of Goldsmith's account activity techniques to digital credential usage information would be obvious to one of ordinary skill, the rejection amounts to hindsight-based reconstruction of the applicant's claims. The rejection thus

neglects both the requirement that a suggestion to combine the references in the manner claimed must be *founded in the prior art*, and that requirement that the *entirety of the teachings of the art (e.g., Musgrave, credit card transactions) must be considered* when formulating a rejection.

It is therefore respectfully submitted that claim 42 is patentable over Goldsmith. Accordingly, it is respectfully submitted that claim 42 and the claims dependent therefrom are allowable.

Independent Claim 42

Independent claim 48 was rejected under 35 U.S.C. § 103(a) as obvious over Goldsmith and Vance.

Claim 48 relates to a method that includes receiving transaction requests from a plurality of delegate users who are delegated from an owner, processing the transaction requests, and communicating transaction information to a central service. The transaction information includes the digital credentials of the delegates. The transaction information is communicated to create, for the plurality of delegate users, activity reports regarding the usage of the digital credentials.

In rejecting claim 48, the action contends that col. 2, line 55-60 of Goldsmith deals with transaction requests that include digital credentials.

Applicant respectfully disagrees. The cited portion of Goldsmith deals with secured passwords. Goldsmith expressly states that these passwords are associated with and allow an individual to access specific bank or investment accounts. See, e.g., col. 2, line 53 (providing *access to an account* over a transaction device 4) and col. 1, line 15-19 ("If the user provides the correct password, … financial transactions for those accounts to which the token permits access [is permitted]"). *See also* col. 2, line 5-8 ("The present invention provided a system for immediately notifying a user of *account activity with respect to one of the user's financial accounts.*") (emphasis added).

Since the passwords are associated with specific bank or investment accounts, Applicant respectfully submits that they are not digital security mechanisms associated with a user's identity. Rather are associated with an account and outside the scope of claim 48. As such, Goldsmith fails to describe or suggest communicating transaction information including digital credentials to create activity reports regarding the usage of the digital credentials.

Vance also fails to describe or suggest such communication. Vance has nothing to do with digital credentials. Hence, no transaction information that includes digital credentials of delegates is communicated to create activity reports.

Moreover, as discussed above, it is respectfully submitted that account identification information is distinct from digital credentials associated with a user's identity. Handling both in the same way is not obvious, especially in light of express teachings in the art of record that they are to be treated differently.

As a result of these distinctions, Goldsmith and Vance fail to describe or suggest storing or processing use information for a digital credential. Accordingly, it is respectfully submitted that claim 48 and the claims dependent therefrom are allowable.

Independent Claim 53

Independent claim 53 was rejected under 35 U.S.C. §103(a) as obvious. Page 25 of the outstanding Office action indicates that claim 53 is obvious over Anderson and Goldsmith. The discussion on page 26 refers to U.S. Patent No. 5,659,616 to Sudia (hereinafter "Sudia"). To advance prosecution, Applicant now responds to rejections under 35 U.S.C. § 103(a) over the

combination of Anderson and Goldsmith and over the combination of Anderson, Goldsmith, and Sudia.

Claim 53 relates to a method that includes receiving a request from a medical professional to access medical information at a remote service, communicating transaction information describing the access request and the digital credential to a credential verification service, receiving a verification result from the credential verification service, providing the medical professional access to the medical information based on the verification result, and receiving an activity report from the credential verification service. The request includes a digital credential for the medical professional. The digital credential is a digital security mechanism associated with the medical professional's identity. The activity report lists the transaction information, the digital credential and the transaction result.

The rejection of claim 53 is respectfully traversed.

In particular, none of Anderson, Goldsmith, and Sudia describe or suggest receiving an activity report that lists transaction information, a digital credential, and a transaction result from a credential verification service to which transaction information is communicated and from which a verification result is received. The rejection admits that

Anderson does not describe or suggest receiving such an activity report from a credential verification service.

Sudia describes that only an acceptance or a rejection of a signature and attribute values is received from a verifier. See, e.g., FIGS. 6, 7, and 8 of Sudia where acceptances 612, 721, 723, 812 and rejections 611, 720, 722, 810 are illustrated in the alternative and the associated description thereof where the operation of Sudia's verifiers is described. It is respectfully submitted that Sudia lacks any description or suggestion of receiving an activity report including anything other than an acceptance or rejection from a credential verification service.

Goldsmith is also silent as to receiving an activity report that lists transaction information, a digital credential, and a transaction result from a credential verification service as claimed. As discussed above, Goldsmith has nothing to do with digital credentials.

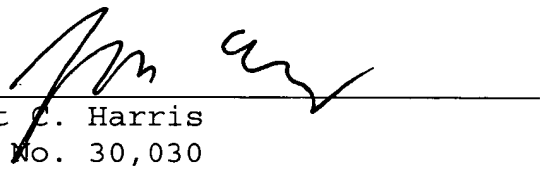
Since none of none of Anderson, Goldsmith, and Sudia describe or suggest receiving an activity report that lists transaction information, a digital credential, and a transaction result from a credential verification service to which transaction information is communicated and from which a verification result is received, it is respectfully submitted

that a prima facie case of obviousness has not been established. Accordingly, it is respectfully submitted that claims 53, and the claims dependent therefrom, are allowable.

Applicant asks that all claims be allowed. No additional claims fees are believed to be due at this time. Please apply any charges not covered or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: September 1, 2004



Scott C. Harris
Reg. No. 30,030
Attorney for Intel Corporation

By John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
PTO Customer Number: **20985**
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10405448.doc